PTO/SB/33 (07-05)
United States Patent & Trademark Office; U.S. DEPARTMENT OF COMMERCE

PRE-APPEAL BRIEF REQUEST FOR REVIEW	Docket Number (Optional) 059864.00876
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on ____________ Signature ____________ Typed or printed Name ____________	Application Number: 10/748,845 Filed: December 29, 2003
	First Named Inventor: Jeremey BARRETT et al.
	Art Unit: 2145 Examiner: Bhatia, Ajay M.

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a Notice of Appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

□ Applicant/Inventor.

□ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed

☒ Attorney or agent of record.
Registration No. 51,091

□ Attorney or agent acting under 37 CFR 1.34.
Reg. No. is acting under 37 CFR 1.34 ________

____
Signature

David E. Brown
Typed or printed name

(703) 720-7800
Telephone number

August 16, 2007
Date

NOTE: Signatures of all of the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

□ *Total of _____ forms are submitted.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:	Confirmation No.: 2762
Jeremey BARRETT et al.	Art Unit: 2145
Application No.: 10/748,845	Examiner: Bhatia, Ajay M.
Filed: December 29, 2003	Attorney Dkt. No.: 59864.00876

For: SYSTEM AND METHOD FOR MANAGING A PROXY REQUEST OVER A SECURE NETWORK USING INHERITED SECURITY ATTRIBUTES

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

August 16, 2007

Sir:

In accordance with the Pre-Appeal Brief Conference Pilot Program guidelines set forth in the July 12, 2005 Official Gazette Notice, Applicants hereby submit this Pre-Appeal Brief Request for Review of the final rejections of claims 1-28 in the above identified application. Claims 1-28 were finally rejected in the Office Action dated March 16, 2007. Applicants filed a Response to the Final Office Action on July 16, 2007, and the Office issued an Advisory Action dated July 24, 2007 maintaining the final rejections of claims 1-28. Applicants hereby appeal these rejections and submit this Pre-Appeal Brief Request for Review.

The Office Action rejected claims 1-28 under 35 U.S.C. 102(b) as being anticipated by US Patent Publication No. 2002/0038371 to Spacey (Spacey).

Applicants respectfully submit that the Office Action failed to establish *prima facie* anticipation because Spacey fails to disclose or suggest all of the features recited in any of the pending claims. This failure constitutes clear error in the Office Action.

Claim 1, from which claims 2-6 depend, is directed to a network device for managing a communication over a network. A transceiver is configured to send and to receive the communication over the network. A processor, coupled to the transceiver, is configured to receive a proxy request from a client through a secure tunnel. The processor is further configured to modify the proxy request to include a security attribute inherent from the secure tunnel. The modified proxy request is forwarded to a proxy service. The security attribute enables a proxy connection through the secure tunnel.

Claim 7, from which claims 8 and 9 depend, is directed to an apparatus for managing a communication over a network. A transceiver is configured to send and to receive the communication over the network. A processor, coupled to the transceiver, is configured to establish a secure tunnel between the apparatus and a client. A proxy request is received from the client through the secure tunnel. The proxy request is modified to include a security attribute inherent from the secure tunnel. The modified proxy request is forwarded to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel.

Claim 10, from which claims 11-17 depend, is directed to a method for managing a communication over a network. A proxy request is received from a client through a secure tunnel. The proxy request is modified to include a security attribute. The modified proxy request is forwarded to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel.

Claims 18, from which claims 19-26 depend, is directed to a system for managing a communication over a network. A client is configured to determine a secure tunnel, and send a proxy request through the determined secure tunnel. A server, coupled to the client, is configured to receive the proxy request from the client through the secure tunnel, and modify the proxy request to include a security attribute inherent from the secure tunnel. The server is further configured to forward the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel.

Claim 27, from which claim 28 depends, is directed to an apparatus for managing a communication over a network. A transceiver arranged to send and to receive the communication over the network. A processor, coupled to the transceiver, is configured to receive a proxy request from a client through a secure tunnel. A means for modifying the proxy request is configured to include a security attribute inherent from the secure tunnel. The apparatus further includes a means for forwarding the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel.

Applicants submit that each of the pending claims recites features that are neither disclosed nor suggested in Spacey.

As discussed in previous correspondence, Spacey is directed to a method allowing communications to pass between private network segments without the need for holes in the firewalls of those networks. The method uses an intermediary machine located somewhere on a public network as described herein. A component in the private service network opens one or more outbound connections to the Intermediary and leaves these connections open waiting for a response. These outbound connections pass transparently through any restrictive firewalls on the private service network since these firewalls are typically set-up to block only unprompted inbound requests. A component on the client private network then connects to the same Intermediary with an outbound connection and sends it a request that should be serviced by a server located on the otherwise inaccessible private service network. The Intermediary passes this client request on to the private service network as a response to the waiting outbound connection previously opened by the service network component to the Intermediary. The client request thus enters the private service network a response to a previously opened outbound connection from the service component and so, is not blocked by the private service networks firewall. The service component reformats the request and transmits it on to the service machine in the private network as required.

Applicants respectfully submit that Spacey fails to disclose or suggest at least the features of "modifying the proxy request to include a security attribute and forwarding the modified proxy request to a proxy service, wherein the security attribute enables a proxy connection through the secure tunnel", as recited in claim 1 and similarly recited in claims 7, 10, 18, and 27.

As discussed in previous correspondence, most notably the Response that was filed on July 16, 2007, Spacey merely discloses an optional encapsulation of the datagram client request in a network packet that is routable to the intermediary, wherein the client sends a network layer request to the address of the destination service application located on a different network element or subnet. See Figs. 6 and 8 and paragraphs [0122] – [0127]. Thus, Spacey does not disclose or suggest modifying the datagram with a security attribute inherent from the secure tunnel, and then forwarding a modified datagram. In other words, in Spacey, the datagram is not modified with the security attribute while passing through the secure tunnel, then forwarded to the proxy service. This omission constitutes clear error in the Office Action.

In the "Response to Arguments" section, the Office Action cites paragraph [0016] of Spacey. However, paragraph [0016] of Spacey merely mentions that Spacey "differs from any existing VPN including (. . . L2F, L2TP . . .) in that communication is via an intermediary and in that, the proxy client and optional modified router component, are preferably required on each network or machine".

Applicants submit that Spacey does not disclose or suggest the features mentioned above because the deficiency still remains that the datagram is not modified with the security attributes while passing through the secure tunnel, then forwarded to the proxy service, as clearly recited in the pending claims. This deficiency is further evidenced in that Spacey is teaching away from the use of a L2TP encapsulation because of its use of an intermediary (See [0016] and also paragraphs [0122] – [0124] of Spacey).

Additionally, MPEP 2131 states that "to anticipate a claim, the references must teach every element of the claim". This principle has been stated by the Federal Circuit: "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628,631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). However, the Office Action essentially does not address the element "modifying the datagram with a security attribute inherent from the secure tunnel, and then forwarding a modified datagram" because it essentially took the position that allegedly Spacey performs the same function. However, as discussed above, this is clearly not the case. Accordingly, for this additional reason, Applicants submit that the Office Action is in clear error.

As discussed in previous correspondence, because claims 2-6, 8, 9, 11-17, 19-26 and 28 depend from claims 1, 7, 10, 18 and 27, these claims are allowable at least for the same reasons as claims 1, 7, 10, 18 and 27, as well as for the additional features recited in these dependent claims.

At least for the reasons discussed above, Applicants submit that the Office Action failed to establish *prima facie* anticipation because Spacey failed to disclose or suggest all of he features recited in any of the pending claims. This failure constitutes clear error in the Office Action.

Reconsideration and withdrawal of the rejections, in view of the clear errors in the Office Action, is respectfully requested. In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

David E. Brown
Registration No. 51,091

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800; Fax: 703-720-7802

DEB:jkm

Enclosures: PTO/SB/33 Form
Notice of Appeal
Petition for Extension of Time
Check No. 16922